UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/491,727	01/27/2000	David M. Austin	AUZ-001 P	8984

7590   09/14/2004

Wesley L Austin esq
1987 South Bluebell drive
Bountiful, UT 84010

EXAMINER
ZIA, SYED

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 09/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _17 May 2004_.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-32_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-32_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on May 17, 2004. Original application contained Claims 1-32. Applicant amended the abstract, and filed substitute drawings. The amendment filed have been entered and made of record. Previous objection to drawings and specification has been withdrawn. Presently pending claims are 1-32.

Response to Arguments

Applicant's arguments filed on May 17, 2004 have been fully considered but they are not persuasive because of the following reasons:

Regarding Claims 1-32 applicants argued that the system of cited prior arts (CPA) [Drake] does not teach, " accessing instructions that access observer data, the observer data including data … and also operating to create data from the observing of the observer Program", "reading instructions that tread memory of the computer system to obtain memory data", "comparing instructions that compare the observer data with memory data read in from memory to determine… computer system, "generating instructions that … whether the observer program is present on the computer system; and "outputting instructions that obtain the results and provide the results for a user".

This is not found persuasive. CPA teaches system and method computer software authentication, protection and security method that involves replacing code with is vulnerable to eavesdropping with equivalent code with vulnerability removed which communicates with hardware and

disables interrupts. The software security method involves using anti-spy techniques within the input routine, which prevent or hamper eavesdropping on the ID-Data. Tamper detection techniques are used within or accessed by the software to disallow the subsequent entry of ID-Data into input routines is tampering is detected. Code, which is vulnerable to eaves dropping, is replaced with equivalent code with the vulnerability removed. The equivalent code communicates directly with the hardware of the computer while disabling system interrupts or other functions, which would permit rouge software to eavesdrop. Therefore, the system of CPA teaches security of computer software, automatically detects tampering of software and code, prevents decompilation reverse engineering, and disassembly, and also prevents executing tracing and debugging by use of code designed to detect and prevent these operations.

As a result, CPA does implement and teaches a system and method for detecting the presence of a computer program for monitoring a user's computer activities and countermeasures against such computer software.

Applicants clearly have failed to explicitly identify specific claim limitations, which would define a patentable distinction over prior arts.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. The examiner will not interpret to read narrowly the claim language to read exactly from the specification, but will interpret the claim language in the broadest reasonable interpretation in view of the specification. Therefore, the examiner asserts that CPA does teach or suggest the subject matter broadly recited in independent and subsequent dependent claims. Accordingly, rejections for Claims 1-32 are respectfully maintained.

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this
> or a foreign country, before the invention thereof by the applicant for a patent.

2.   Claim 1-32 are rejected under 35 U.S.C. 102(a) as being anticipated by Drake (U.S.

Patent No. 6,006,328). With respect to claim 1, Drake teaches a system for detecting an

observing program on a computer system (see abstract; col. 3, lines 32-44), the system

comprising:

accessing instructions that access observer data, the observer data including data

descriptive of an observer program, the observer program being programmed to observe a

user's activities on the computer system and also operating to create data from the

observing of the observer

program (see col. 3, lines 32-67);

reading instructions that tread memory of the computer system to obtain memory data

(see col. 4, lines 47-65; col. 6, lines 10-20)

comparing instructions that compare the observer data with memory data read

in from memory to determine whether the observer program is present on the computer system

(see col. 6, lines 5-48);

generating instructions that generate results from the comparing, wherein the

results generated indicate whether the observer program is present on the computer system (see

col. 6, lines 5-48); and

outputting instructions that obtain the results and provide the results for a user (see col. 4,

lines 47-65; col. 6, lines 5-48).

3.   Claim 2 is rejected as above in rejecting claim 1, wherein the reading instructions read

the memory of the computer system by querying the operating system of the computer system

for the tasks running and by examining task information provided by the operating system (see

col. 3, lines 32-67).

4.   Claim 3 is rejected as above in rejecting claim 1, wherein the outputting instructions

provide the results to a user through a graphical user interface (see col. 9, lines 8-14; col. 10,

lines 12-16).

5.   Claim 4 is rejected as above in rejecting claim 1, wherein the reading instructions read

the memory of the computer system by querying the file system of the computer system for the

files located on storage media and by examining file information provided by the file system (see

col. 6, lines 7-20).

6.   Claim 5 is rejected as above in rejecting claim 1, wherein the reading instructions read

the memory of the computer system by opening a file located on storage media and by

examining contents of the file (see col. 6, lines 10-20).

7.   Claim 6 is rejected as above in rejecting claim 1, wherein the observer data includes data

descriptive of a plurality of observer programs and wherein the system compares the observer

data with the memory data to determine whether any known observer program is present (see

col. 6, lines 7-48).

8.   Claim 7 is rejected as above in rejecting claim 1, further comprising countermeasure instructions wherein the countermeasure instructions alter the operation of the observer program (see col. 3, lines 46-52).

9.   Claim 8 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by altering observer program configuration data (see col. 4, lines 47-65; col. 8, lines 3-12).

10.   Claim 9 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by altering a file on the computer system (see col. 7, lines 12-23; col. 8, lines 3-12).

11.   Claim 10 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by altering reporting data generated by the observer program (see col. 5, lines 20-34; col. 7, lines 53-67 to col. 8, lines 1-12).

12.   Claim 11 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by replacing reporting data generated by the observer program (see col. 5, lines 38-62).

13.   Claim 12 is rejected as above in rejecting claim 7, wherein the countermeasure instructions alter the operation of the observer program by replacing a file of the observer program (see col. 5, lines 20-34).

14.   Claim 13 is rejected as above in rejecting claim 1, wherein the observer data includes data descriptive of observing activity typical of observing programs and wherein the system compares the observer data with the memory data to determine whether any known observer program is present (see col. 6, lines 5-48).

15.   Claim 14 is rejected as above in rejecting claim 1, further comprising the observer data,

wherein the observer data includes a list of files and modules that are part of the observer

program software, and wherein the reading instructions read the memory of the computer system

by querying the operating system of the computer system for the tasks running and by examining

task information provided by the operating system, and wherein the reading instructions also

read the memory of the computer system by querying the file system of the computer system for

the files located on storage media and by examining file information provided by the file system,

and wherein the outputting instructions provide the results to a user through a graphical user

interface (see col. 3, lines 32-57; col. 4, lines 47-65; col. 6, lines 5-48).

16.   Claim 15 is rejected as above in rejecting claim 1, wherein the system is made available

over a computer network through a web site (see col. 13, lines 28-34).

17.   With respect to claim 16, Drake teaches a system for detecting an observing program on a

computer system (see abstract; col. 3, lines 32-44), the system comprising:

        means for accessing observer data, the observer data including data descriptive of an

observer program, the observer program being programmed to observe a user's activities on the

computer system and also operating to create data from the observing of the observer program

(see col. 3, lines 32-67);

        means for reading memory of the computer system to obtain memory data (see col. 4,

lines 47-65; col. 6, lines 10-20).

        means for comparing the observer data with memory data to determine whether the

observer program is present on the computer system (see col. 6, lines 5-48);

means for generating results from the comparison, wherein the results generated indicate whether the observer program is present on the computer system (see col. 6, lines 5-48); and

means for outputting the results for a user see col. 4, lines 47-65; col. 6,lines 5-48).

18.   With respect to claim 17, Drake teaches a method for detecting an observing program on a computer system (see abstract; col. 3, lines 32-44), the method comprising the steps of:

accessing observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3, lines 32-67);

reading memory of the computer system to obtain memory data (see col. 4,lines 47-65; col. 6, lines 10-20);

comparing the observer data with memory data read in from memory to determine whether the observer program is present on the computer system (see col. 6, lines 5-48);

generating results from the reading and comparing, wherein the results generated indicate whether the observer program is present on the computer system (col. 6, lines 5-48); and

outputting the results for a user (see col. 4, lines 47-65; col. 6, lines 5-48).

19.   With respect to claim 18, Drake teaches a computer-readable medium containing instructions for detecting an observing program on a computer system (see abstract; col. 3, lines 32-44), wherein the instructions comprise executable instructions for implementing a method comprised of the steps of:

accessing observer data, the observer data including data descriptive of an observer

program, the observer program being programmed to observe a user's activities on the computer

system and also operating to create data from the observing of the observer program (see col.

3,lines 32-67);

reading memory of the computer system to obtain memory data (see col. 4,lines 47-65;

col. 6, lines 10-20);

comparing the observer data with memory data read in from memory to determine

whether the observer program is present on the computer system (see col. 6, lines 5-48);

generating results from the reading and comparing, wherein the results generated indicate

whether the observer program is present on the computer system (see col. 6, lines 5-48); and

outputting the results for a user (see col. 4, lines 47-65; col. 6, lines 5-48).

20.   Claim 19 is rejected as above in rejecting claim 18, wherein the computer-readable

medium is a data transmission medium (see col. 13, lines 27-33).

21.   With respect to claim 20, Drake teaches a system for altering the operation of an observer

program on a computer system, the system comprising (see abstract; col. 3, lines 32-44; col. 4,

lines 47-65):

accessing instructions that access observer information, the observer information

including data descriptive of the observer program, the observer program being programmed to

observe a user's activities on the computer system and also operating to create data from the

observing of the observer program (see col. 3,lines 32-67);

reading instructions that read memory of the computer system to obtain files relating to

the observer program (se col. 4, lines 47-65; col. 6, lines 10-20);

altering instructions that alter a file relating to the observer program such that the

operation of the observer program is changed (see col. 5, lines 42-62; col. 8, lines 3-12).

22.   Claim 21 is rejected as above in rejecting claim 20, comprising an observer detection

program (see col. 3, lines 32-44).

23.   Claim 22 is rejected as above in rejecting claim 20, further comprising inputting

instructions that display to a user options regarding the altering and that take input from the user

relating to the options (see col. 11, lines 30-46).

24.   Claim 23 is rejected as above in rejecting claim 20, wherein the altering instructions alter

the operation of the observer program by altering observer program configuration data (see col.

4, lines 47-67 to col. 5, lines 1-14; col. 6, lines 21-31).

25.   Claim 24 is rejected as above in rejecting claim 20, wherein the altering instructions alter

the operation of the observer program by altering a file on the computer system (see col. 4, lines

47-67 to col. 5, lines 1-14)

26.   Claim 25 is rejected as above in rejecting claim 20, wherein the altering instructions alter

the operation of the observer program by altering reporting data generated by the observer

program (see col. 4, lines 47-65; col. 5, lines 37-58).

27.   Claim 26 is rejected as above in rejecting claim 20, wherein the altering instructions alter

the operation of the observer program by replacing reporting data generated by the observer

program (see col. 4, lines 47-65; col. 5, lines 37-58).

28.   Claim 27 is rejected as above in rejecting claim 20, wherein the altering instructions alter the operation of the observer program by replacing a file of the observer program (see col. 4, lines 47-65; col. 5,lines 37-58).

29.   Claim 28 is rejected as above in rejecting claim 20, wherein the system is made available over a computer network through a web site (see col. 13, lines 27-33).

30.   With respect to claim 29, Drake teaches a system for altering the operation of an observer program on a computer system (see abstract; col. 3, liens 32-44; col. 4, lines 47-65), the system comprising:

    means for accessing observer information, the observer information including data descriptive of the observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program (see col. 3, lines 32-67);

    means for reading memory of the computer system to obtain files relating to the observer program (see col. 4, lines 47-67; col. 6, lines 10-20); and

    means for altering a file relating to the observer program such that the operation of the observer program is changed (see col. 5, lines 42-62; col. 8, lines 3-12).

31.   With respect to claim 30, Drake teaches a method for altering the operation of an observer program on a computer system (see abstract; col. 3, lines 32-44; col. 4, lines 47-65), the method comprising the steps of:

    accessing observer information, the observer information including data descriptive of the observer program, the observer program being programmed to observe a user's activities on

the computer system and also operating to create data from the observing of the observer

program (see col. 3, lines 32-67);

reading memory of the computer system to obtain files relating to the observer

program (see col. 4, lines 47-67; col. 6, lines 10-20) and

altering a file relating to the observer program such that the operation of the

observer program is; changed (see col. 5, lines 42-62; col. 8, lines 3-12).

32.   With respect to claim 31, Drake teaches a computer-readable medium containing

instructions for altering the operation of an observer program on a computer system, wherein the

instructions comprise executable instructions for implementing a method comprised of the steps

of:

accessing observer information, the observer information including data descriptive of

the observer program, the observer program being programmed to observe a user's activities on

the computer system and also operating to create data from the observing of the observer

program (see col. 3, lines 32-67);

reading memory of the computer system to obtain files relating to the observer

program (see col. 4, lines 47-65; col. 6, lines 10-20); and

altering a file relating to the observer program such that the operation of the

observer program is changed (see col. 5, lines 42-62; col. 8, lines 3-12).

33.   Claim 32 is rejected as above in rejecting claim 31, wherein the computer-readable

medium is a data transmission medium (see col. 13, lines 27-33).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the mailing

date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Syed Zia whose telephone number is 703-305-3881. The

examiner can normally be reached on Monday - Friday 9:00 AM to 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

sz
September 08, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100